MEMORANDUM OF UNDERSTANDING BETWEEN
THE CANADIAN PUBLIC ACCOUNTABILITY BOARD
AND
THE FINANCIAL REPORTING COUNCIL
ON COOPERATION AND THE EXCHANGE OF INFORMATION
RELATED TO THE OVERSIGHT OF AUDITORS

The Canadian Public Accountability Board ("CPAB"), based on its obligations and authority under Canadian federal and applicable provincial laws

and

the Financial Reporting Council ("FRC"), based on its obligations and authority under applicable legislation including the Companies Act 2006 and the Statutory Audit and Third Country Auditor Regulations 2016

Recognising that the European Commission has decided upon the equivalence referred to in Article 46, paragraph 1 of Directive 2006/43/EC in respect of Canada[1],

Recognising that the European Commission has decided upon the adequacy referred to in Article 47, paragraph 1(c) of Directive 2006/43/EC in respect of Canada[2], enabling the exchange of audit working papers between the EU Member States' oversight authorities and Canada,

Recognising that the transfer of data from the United Kingdom to Canada must be in accordance with the Data Protection Act 1998 implementing Directive 95/46/EC, and in particular Chapter IV of Directive 95/46/EC,

Recognising that the European Commission has determined the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act[3],

have agreed as follows:

---

[1] Commission Decision No 2011/30/EU of 19 January 2011
[2] Commission Decision No 2010/64/EU of 5 February 2010
[3] Commission Decision No. 2002/2/EC of 20 December 2001

PURPOSE

1. Both Parties seek to improve the quality, accuracy and reliability of the audit of public companies through audit regulation and auditor oversight so as to protect investors, help strengthen public trust in the audit process and increase investor confidence in their respective capital markets. Given the global nature of capital markets, the Parties recognise that it is in their common interest to cooperate in the oversight of auditors that fall within the regulatory jurisdiction of both Parties, to the extent such cooperation is compatible with the Parties' respective Laws and/or Regulations, their important interests and their available resources. They also recognise the importance of cooperation to avoid an undue burden on audit firms of overlapping supervision.

2. The purpose of this MOU is to facilitate cooperation between the Parties to the extent permitted by their respective national laws in the area of public oversight, registration, inspections and investigations of Auditors of companies that are subject to the regulatory jurisdiction of both the CPAB and the FRC.

DEFINITIONS

3. For the purpose of this MOU,

   "Auditor" or **"Auditors"** means a natural person or an audit firm that is subject to the oversight of both Parties in accordance with the Companies Act 2006 in the UK and National Instrument 52-108 – Auditor Oversight in Canada;

   "Audit Working Papers and **Investigation Reports"** means any documents which are or have been held by a statutory auditor within the regulatory jurisdiction of the Parties, which are related to the conduct of an audit conducted by that Auditor; any report of an inspection of the conduct of an audit by a statuory auditor within the jurisdiction of the Parties; or any report of an investigation into the conduct of a statutory auditor within the regulatory jurisdiction of the Parties.

   "Information" refers to public and non-public information and/or documents which includes but is not limited to:

   1) reports on the outcome of inspections , including information on firm-wide procedures and engagement reviews;
   2) Audit Working Papers or other documents held by Auditors;
   3) Investigation Reports; and
   4) information relating to other areas of mutual interest for the purpose of supervision,

provided that the information relates to matters that are subject to the regulatory jurisdictions of both Parties[4].

"**Inspections**" refers to external quality assurance reviews of Auditors generally undertaken on a regular basis with the aim of enhancing audit quality.

"**Investigations**" refers to investigations in response to a specific suspicion of infringement or violation of Laws and/or Regulations.

"**Laws and/or Regulations**" means any laws, rules or regulations in force in the respective countries of the Parties;

"**Party**" or "**Parties**" means CPAB and/or the FRC.

COOPERATION

Mutual recognition

4. The Parties may rely on the supervision of the Auditors in their home country and may choose to refrain from public oversight activities, inspections, investigations and penalties with respect to Auditors from the other country on the basis of reciprocity, to the extent permitted by their respective Laws and/or Regulations.

5. The Parties may endeavour to minimise the burden related to the registration of Auditors from the other country on the basis of reciprocity, to the extent permitted by their respective Laws and/or Regulations.

6. Cooperation may include one Party assisting the other Party in an inspection or an investigation by performing activities that may include but are not limited to facilitating access to information and/or, if requested, reviewing audit work papers and other documents.

---

[4] For the avoidance of doubt:

- CPAB is also able to provide documents or information that a Canadian auditor obtained or prepared in order to perform the audit of a Canadian reporting issuer that carries on business in the FRC's jurisdiction to the FRC if they relate to the FRC's review of an audit carried out on such Canadian reporting issuer (as per section 14 of the Canadian Public Accountability Board Act (Ontario) 2006) even if such Canadian auditor is not directly registered with the FRC. This does not include privileged documents, privileged information or information based on privileged information.
- The FRC is able to transfer to CPAB audit working papers or other documents held by a UK statutory audit firm if they relate to the audit of a company that has issued securities in Canada or which forms part of a Group issuing statutory consolidated accounts in Canada (as per Section 1253DA of the Companies Act 2006), even if such UK audit firm is not directly registered with CPAB.

Scope of cooperation

7. Cooperation includes the exchange of Information for the purpose of facilitating cooperation in the area of public oversight, registration, inspections and investigations of Auditors, to the extent permitted or required by Laws and/or Regulations.

8. A Party shall endeavour to inform the other Party, within a reasonable amount of time, of a sanction or disciplinary measure it has imposed on an Auditor that falls within the regulatory jurisdiction of both Parties and which relates to a systemic defect in the quality of the audit work of such Auditor.

9. In cases where the Information requested may be maintained by or available from another authority within the country of the requested Party, the requested Party will endeavour to provide the Information requested, to the extent permitted by Laws and/or Regulations.

Requests for information

10. Requests will be made in writing (including e-mail) and be addressed to the contact person of the requested Party.

11. The requesting Party should specify the following:

    (a) The Information requested;
    (b) The purposes for which the Information will be used[5];
    (c) The reasons why the Information is needed and, if applicable, the respective Laws and/or Regulations that may have been violated;
    (d) An indication of the date by which the Information is needed; and
    (e) An indication, to the best of the knowledge of the requesting Party, whether the Information requested might be subject to further use or disclosure under paragraphs 24 to 27.

12. Any request for information which is held exclusively by the relevant Auditor shall be made to the other Party and not directly to the relevant Auditor.

[5] In accordance with Section 1253E of the Companies Act 2006, it is only permissible for the FRC to request, transfer, or agree to the transfer of, Information in connection with the functions of (i) quality assurance of Auditors; (ii) investigation, discipline and penalty of Auditors; and (iii) public oversight of Auditors.

Execution of requests for non-public information

13. Each Party will provide the other Party with information upon request, subject to paragraph 17 below.

14. Each request will be assessed on a case by case basis by the requested Party to determine whether non-public information can be provided under the terms of this MOU. In any case where the request cannot be met in full within the desired time period, the requested Party will inform the requesting Party accordingly, and will consider whether other relevant information or assistance can be given.

15. Each Party shall endeavour to provide a prompt and adequate response to requests for non-public information.

16. In order to avoid unnecessary delays, the requested Party will provide, as appropriate, parts of the requested non-public information as it becomes available.

17. The requested Party may refuse to act on a request where:

    (a) It concludes the request is not in accordance with this MOU;
    (b) Acceding to the request would contravene the Laws and/or Regulations of the requested Party's country or where such non-public information is covered by solicitor/attorney-client privilege or legal professional privilege under the Laws and/or Regulations of the requested Party's country;
    (c) It would burden the requested Party disproportionately;
    (d) It concludes it would be contrary to the public interest of the requested Party's country for assistance to be given;
    (e) The provision of non-public information would adversely affect the sovereignty, security or public order of the requested Party's country; or
    (f) Judicial proceedings (civil, criminal or administrative proceedings)have already been initiated, or have become legally effective, in respect of the same actions and against the same persons before the authorities of the country of the requested Party; or
    (g) the protection of the commercial interst of any audited person, including industrial and intellectual property, is undermined.

18. The requested Party will promptly inform the requesting Party of the reasons, where it refuses to act on a request made under this MOU.

19. Any non-public document or other material provided in response to a request under this MOU and any copies thereof shall be returned on request to the extent permitted by the applicable domestic Laws and/or Regulations.

CONFIDENTIALITY

20. Each Party shall keep confidential all non-public information received or created in the course of cooperating in accordance with the terms of this MOU, subject to paragraphs 24 to 28. The obligation of confidentiality shall apply to all persons who are or have been:

    (a) employed by the Parties;
    (b) involved in the governance of the Parties; or
    (c) otherwise associated with the Parties.

21. The Parties have established and will maintain such safeguards as are necessary and appropriate to protect the confidentiality of the information, including storing the information in a secure location when not in use.

22. The Parties have provided each other a description of their applicable information systems and controls and a description of their Laws and/or Regulations that establish appropriate limits on access to non-public information.

23. The Parties will inform each other if the safeguards, information systems, controls, laws or regulations referred to in paragraphs 21 and 22 above change in a way that weaken the confidentiality of the information and/or documents provided by the other Party.

USE OF NON-PUBLIC INFORMATION

24. The Parties may use non-public information received or created in the course of cooperation *only* for the exercise of their functions of public oversight, registration, inspections and investigations of Auditors. If either Party intends to use non-public information received or created in the course of cooperation for any purpose *other* than those stated in the request it must obtain the prior written and specific consent of the requested Party. If the requested Party consents to the use of non-public information for a purpose other than that stated, it may subject such use to conditions.

EXCEPTIONS TO CONFIDENTIALITY

25. In the event that the requesting Party is required to disclose or to transfer non-public information received or created in the course of cooperation, in order to comply with its

obligations under its Laws and/or Regulations, by a court order, or when legally obligated to onward share with a relevant regulatory authority or professional regulatory authority, it will provide, wherever possible, at least fifteen working days written notice to the requested Party or such period as is reasonable and available in the circumstances prior to its disclosure or transfer, stating the reasons as to why it is required to disclose or to transfer the Information.

26. If the requested Party objects to the disclosure or transfer of such non-public information received or created, the requesting Party will make its best efforts to resist the disclosure or transfer of the non-public Information received or created.

27. A Party may publicly announce its sanctions or disciplinary measures imposed on Auditors that fall within the regulatory jurisdiction of both CPAB and the FRC, as permitted or required by Laws and/or Regulations of that Party's jurisdiction. Before making public any sanctions or disciplinary measures imposed on an Auditor that is located in the other Party's jurisdiction, the Party intending to announce the sanctions or disciplinary measures shall use reasonable endeavours to give reasonable advance written notice to the other Party prior to the announcement.

28. A Party that intends to disclose or to transfer to a third party non-public Information received or created, other than in cases referred to in paragraph 25, must obtain the prior written and specific consent of the Party which provided the non-public Information. The Party which intends to disclose or to transfer the non-public Information shall give the reasons and the purposes for which it would be disclosed or transferred. The requested Party may make its consent to the disclosure of the non-public Information subject to conditions.

THE TRANSFER OF PERSONAL DATA

29. The Parties will only transfer personal data in accordance with their respective Laws and/or Regulations.

OTHER

30. This MOU does not create any binding legal obligations, nor does it modify or supersede any Laws and/or Regulations in Canada or in the UK. This MOU does not give rise to a right on the part of CPAB, the FRC or any other governmental or non-governmental entity or any private

person to challenge, directly or indirectly, the degree or manner of cooperation by CPAB or the FRC.

31. This MOU does not prohibit the Parties from taking measures with regard to the supervision of Auditors that are different from, or in addition to, the measures set forth in this MOU.

32. The Parties shall, at the request of either Party, consult on issues related to the matters covered by this MOU, and otherwise exchange views and share experiences and knowledge gained in the discharge of their respective duties, to the extent permitted by their respective Laws and/or Regulations.

33. The Parties may consult informally, at any time, about a request or proposed request or about any Information provided.

34. The Parties may consult and revise the terms of this MOU in the event of a substantial change in the Laws and/or Regulations, or practices affecting the operation of this MOU, or if they wish to modify the terms of their cooperation.

ENTRY INTO EFFECT AND TERMINATION

35. This MOU will come into force from the date of signature by both Parties.

36. This MOU may be terminated by either Party at any time upon giving at least thirty days prior written notice to the other Party. The provisions concerning confidentiality (paragraphs 20 to 28) and on the transfer of personal data shall remain in force thereafter.

For the Canadian Public Accountability Board

Brian A. Hunt
Chief Executive Officer
Date: Nov. 30, 2016

For the Financial Reporting Council

M McLaren

Melanie McLaren
Executive Director of Audit and Actuarial Regulation
Date: 9/12/16

CANADIAN PUBLIC ACCOUNTABILITY BOARD
CONSEIL CANADIEN SUR LA REDDITION DE COMPTES

Privileged & Confidential

To: Foreign Auditor Oversight Bodies

Date: May 2014

Re: CPAB's Confidentiality Regime

The following is a summary of the laws and regulations protecting the confidentiality of documents in CPAB's possession, whether produced internally or received from a foreign auditor oversight body.

Canadian Legislative Scheme:

Securities in Canada are not regulated on a national basis, but on a provincial or territorial basis. The 10 provinces and 3 territories in Canada are responsible for securities regulation and each has its own independent securities regulatory body. Securities regulators from each province and territory form the CSA, which is primarily responsible for developing a harmonized approach to securities regulation across the country.

The CSA enacted CSA National Instrument (NI) 52 – 108 in 2004 to give CPAB its key required powers. This is the main source of CPAB's authority. NI 52-108 requires all Canadian RI's, that is, companies that have raised funds from the Canadian investing public and who, for that reason, must file financial statements with one or more provincial Securities Commissions, to have their financial statements audited by an auditor that is a participant in CPAB's auditor oversight program (section 4). Likewise, under NI 52-108, accounting firms that audit Canadian RI's must be overseen by, and be participants in, CPAB's auditor oversight program (section 2). NI 52-108 is however silent with respect to confidentiality of documents in CPAB's possession. This instead falls under the jurisdiction of each province in which CPAB operates.

Auditor oversight body legislation has been passed in Quebec, Ontario, British Columbia, Manitoba, Yukon Northwest Territories, Saskatchewan and New Brunswick.

In terms of confidentiality, we operate in accordance with the provisions of the Canadian Public Accountability Board Act (Ontario), 2006, (the "CPAB Act"), as it is the most comprehensive legislation, and its drafters gave careful thought to confidentiality and restrictions in terms of with which third parties CPAB can share information. In addition, as over 90% of all Canadian reporting issuers are Ontario-based or have the Ontario Securities Commission as their "lead" regulator (if the Canadian reporting issuer is subject to the jurisdiction of several securities regulators often one is selected as the lead regulator) it is more often than not the relevant Act which will apply to our actions.

CPAB Act

The CPAB Act provides that all documents and other information prepared for or received by CPAB in the exercise of its mandate in connection with an inspection, investigation or review panel proceeding carried out under CPAB's oversight program, are confidential and may not be disclosed without (a) the written consent of all persons whose interests might reasonably be affected by the disclosure; or (b) a court order authorizing the disclosure. (Section 11(2))

The CPAB Act also provides that our personnel may not be required to give testimony or produce any document or information with respect to documents they are prohibited from disclosing under the Act, except in a proceeding under the Act (an audit firm's appeal of one of our disciplinary rulings). (Section 11(3)) No one has ever attempted to secure access to our materials, or to compel us to testify.

The CPAB Act allows us to notify the Securities Commission, any regulatory authority; any law enforcement agency and any professional regulatory authority if it appears that there may have been a contravention of the law by any person or company. However, the scope of such notification is limited by the caveat that we may not disclose privileged documents or information or any specific information relating to the business , affairs or financial condition of a participating audit firm or any client of a participating firm – unless all parties whose interests might reasonably be affected by the disclosure have consented in writing . Neither may we use privileged information to determine if we have reasonable grounds to suspect a contravention of the law (Section 6 (3) (a) and Section 13).

Finally, even in our Annual Report, the information provided in it is general in nature – we do not discuss particular firms or provide details of where information originated from. The CPAB Act also provides that members of our Council of Governors (which include the heads of the largest Securities Commissions) are not entitled to, and shall not be given access to, any documents or information relating to our specific audit of a reporting issuer (Section 9). In practice this means we don't share firm or client specific information with our Board, or our Council of Governors, or with anyone else, including the Securities Commissions. The only firm specific information that would become available would be with respect to our imposition of a restriction or sanction on a firm – our most severe disciplinary measures.

If we were in receipt of information from a foreign audit oversight body, that information would be protected from disclosure on the basis of the above.

Other Provincial Legislation

All other provincial auditor oversight legislation contains two basic points that protect any information we may receive:

- CPAB and its personnel are non–compellable, and cannot be required to testify or produce information with respect to CPAB's inspections or investigations.

- CPAB is provided with immunity – so long as it is acting in good faith within its mandate.

Rules

The CPAB Rules, which governs CPAB's actions, contain many similar protections as those contained in the CPAB Act.

The Rules stipulate that any documents or other information prepared or received by or specifically for CPAB or CPAB staff in connection with an Inspection of a participating audit firm shall be confidential and in CPAB's hands, provided however that CPAB will, if it considers it appropriate, disclose such information: (i) to any professional regulatory authority having jurisdiction over the participating audit firm or its designated professionals; and (ii) to securities regulators and the Superintendent of Financial Institutions Canada, provided only that disclosure shall not be made of any specific information relating to the business, affairs or financial condition of any client of the participating audit firm except to the extent such disclosure may be authorized by applicable law; and when making such disclosure CPAB shall inform the recipient that the information is confidential (Section 417). These restrictions also apply to Investigations, and any documents, testimony or other information prepared or received by or specifically for CPAB in connection with such Investigations (Section 516).

CPAB may, at any time, publish such summaries, compilations or general reports concerning the procedures, findings and results of its various Inspections as it deems appropriate. However, CPAB will use its best efforts not to publish information that would enable the identification of the firm or firms, unless that information has previously been made public by lawful means, and in practice such generalized reports would not identify if such information was received from a specific foreign audit oversight body (Section 419).

If we were in receipt of information from a foreign audit oversight body, that information would also be protected from disclosure on the basis of the above.

Codes of Ethics

CPAB has enacted a Code of Ethics for its staff members and consultants, and a Code of Ethics for its Board of Directors.

Both Codes prohibit staff members, consultants and Directors from disseminating or disclosing any non-public information obtained in the course of their work or Board membership. This provision continues in effect after the end of their role with CPAB.

Each staff member, consultant and Director confirms annually that they have read and understood the Code of Ethics and will comply with all of its provisions.

Internal Security

All encrypted files received by a foreign audit oversight body are stored on the CPAB infrastructure, which is protected with two separate firewalls. CPAB employee laptops are IP tracked and are secured with a three level password authentication with hard disk encryption. CPAB continually maintains the highest security standards available in Canada regarding its information and data. CPAB's infrastructure is subject to an external security assessment every two years.

Rules applying to the protection of Personal Information and Data legislation in Canada

The federal Personal Information Protection and Electronic Documents Act ("PIPEDA") sets out ground rules for the management of personal information (data) in the private sector. It regulates the collection, use and disclosure of personal information as part of a 'commercial activity'.

CPAB's activities do not fall within the definition of a 'commercial activity'. CPAB is not, therefore, subject to the PIPEDA requirements. In addition, it is extremely unlikely that any of the information we obtain from you would be considered personal information.

Nevertheless, CPAB endeavors in its affairs to meet PIPEDA's standards, and regards the protection of all data collected during inspections and the personal information of its employees, consultants, directors, hearing officers and the designated professionals of its participating firms as essential to the organizations' integrity and reputation. Accordingly, CPAB uses safeguards, controls and procedures to voluntarily comply with PIPEDA standards. In the rare instances where we access personal data or information, the application of our policies and practices should protect the confidentiality of such personal data and information.

Therefore, CPAB complies with PIPEDA on a voluntary basis and has appropriate controls over private and confidential data and information, and would meet such standards in its exchanges with foreign audit oversight bodies. We would notify you immediately if we were unable to provide information due to a restriction on the transfer of personal information or data.

FRC CONFIDENTIALITY AND INFORMATION SECURITY POLICY AND PRACTICES

1. Laws and Regulations Relevant to Access to Information Held by the Financial Reporting Council

Legal Restrictions on Disclosure

1.1. The Companies Act 2006 imposes restrictions on the disclosure of information that relates to the private affairs of an individual or to any particular business that is provided to the Financial Reporting Council (as the designated body for the purposes of section 1252[1]), in connection with its statutory functions for the regulation of statutory auditors, or to the Audit Quality Review team (AQR), as the independent monitoring body.

1.2. Specifically, Section 1224A(3) prohibits the disclosure of any such information not already available to the public without the consent of the individual or person responsible for the business. Sections 1224A(4) and (5) set out the exceptions to that prohibition, that enable the FRC to disclose information it has received in the following cases:

- disclosures to enable the FRC to carry out the functions in Part 42 of the Companies Act 2006. The principal functions are the recognition and oversight, in accordance with the statutory requirements, of accountancy bodies (i) known as Recognised Qualifying Bodies, that offer an audit qualification and/or (ii) known as Recognised Supervisory Bodies, that supervise statutory auditors.

- disclosures made to a person specified in Part 1 of Schedule 11A, a copy of which is attached hereto. This lists a number of public authorities and regulatory bodies as specified persons

- disclosures made for a purpose specified in Part 2 of Schedule 11A, a copy of which is attached hereto. This lists a number of purposes related in the vast majority of cases to statutory regulatory functions

- disclosures to a competent authority in the European Economic Area responsible for the regulation or oversight of auditors, in accordance with Section 1253B; and disclosures to a competent authority in a third country responsible for the regulation or oversight of auditors, in the case of audit working papers, in accordance with specific statutory provisions (see 1.4 to 1.6 below) and, otherwise, for the purposes of enabling that authority to exercise its functions.

1.3. A disclosure made in contravention of these requirements is a criminal offence under section 1224B, with penalties of imprisonment or a fine. Section 1224B provides a defence to the offence where the person did not know and had no reason to suspect that the disclosure had been made, or where the person took all reasonable steps and exercised due diligence to avoid the commission of the offence.

---

[1] The Secretary of State has delegated most of his responsibilities for audit regulation through the Statutory Auditors (Amendment of Companies Act 2006 and Delegation of Functions etc) Order 2012 (SI 2012/1741)

Specific Statutory Provisions in relation to audit working papers

1.4. Section 1253E includes additional restrictions on the disclosure of audit working papers obtained from a third country competent authority or a third country audit firm:

- Section 1253E(3) requires that any working arrangements with third countries must provide that the FRC may not use audit working papers obtained other than in connect with audit regulation (quality assurance, investigation and discipline, public oversight).

- Section 1253E(5) requires that the FRC and persons employed or formerly employed in discharging its statutory functions must be subject to "obligations of confidentiality as to personal data, professional secrets and sensitive commercial information contained in audit working papers transferred [to the FRC]".

Common Law Duty of Confidentiality

1.5. Under common law, that is law applied by the courts by reference to previous cases, the general position in the UK is that, if information is given in circumstances where the recipient owes a duty of confidence or where the information is by its nature "confidential", then that information cannot normally be disclosed without the information provider's consent. There are some circumstances where disclosing otherwise confidential information is lawful, in particular:

- where disclosure is in the overriding public interest;
- where there is a legal duty to do so, for example a court order.

Ability of the FRC to Transfer Confidential Information to Other Entities.

1.6. The legal framework that permits the FRC to transfer otherwise confidential information to other bodies or for specified purposes is set out at 1.2 above. Although there is no statutory provision that only permits transfers where the recipient itself has specified confidentiality arrangements in place, since transfers are permitted only to specified bodies carrying out public interest functions or for specified regulatory functions, there is an expectation that adequate confidentiality arrangements will be in place in the recipient body.

Freedom of Information Act

1.7. The FRC is subject to the Freedom of Information Act 2000 (FOIA) which provides public access to information held by public authorities on the principle that people have a right to know about the activities of public authorities. The FRC is a public authority in respect of its statutory duties delegated to it by the Secretary of State, which includes the regulation of third country auditors. The right of access is subject to a number of exemptions and we would consider the application of the exemptions to any requests in relation to information provided by a foreign authority in the course of providing international assistance. The exemptions likely to apply would include Section 41 which states that information will be exempt if it was obtained from another person or organisation and disclosure would result in a breach of confidence over which a person could take legal action and Section 44(1) (a) which provides for the exemption of information where its disclosure is prohibited by other legislation. Provisions in existing legislation prohibiting the disclosure of information are referred to as

statutory prohibitions or statutory bars and require a public authority not to disclose specific information.

Data Protection

The Data Protection Act 1998 provides for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. Any personal data provided to the FRC must be processed in accordance with the principles set out in the Data Protection Act. Further, section 1224A, subsection (7) makes it clear that the requirements of the Data Protection Act 1998 apply to the disclosure of information by the FRC.

Decision to Transfer Confidential Information

1.8. A decision to transfer confidential information held by the FRC to another person is taken on the merits of the individual case within the legal framework set out above. Any such decision must be made with the approval of the Chair, Conduct Committee and the Executive Director, Conduct Division (the Conduct Division is a part of the FRC), other than in exceptional circumstances.

2. Obligations on Staff and Board members for the maintenance of the confidentiality of non-public information

2.1. The statutory and common law obligations in respect of information disclosure are supplemented by Codes of Conduct and requirements that apply to staff of the FRC and the AQR, and to members of the FRC and its Conduct Committee.

Board Members

2.2. The FRC has a Code of Conduct for all non-executive and executive members of the Board of FRC Ltd and all members of the sub committees of the FRC and this therefore applies to all members of the Conduct Committee and governs the conduct of their work as a Board member. The Code sets out general principles and covers the collective and individual responsibilities of Board Members, conflicts of interest, hospitality and gifts, and confidentiality.

2.3. On the confidentiality of information, the Code states:

All information acquired by Board members in the exercise of their functions as Board members during their appointment is confidential to the FRC and/or its Committees. Board members must not during their appointment or afterwards (unless he or she is authorised by the FRC Chair or the relevant Committees or is under a legal obligation to do so):

I. use for his/her own benefit or the benefit of any other person; or
II. disclose to any person; or
III. through any failure to exercise all due care and diligence, cause or permit any unauthorised disclosure of any confidential information that he or she obtains by virtue of their position as a Board member.

In addition, there is a specific responsibility on Board Members that they must not misuse information gained in the course of their service for personal gain.

2.4. The most likely sanction against a breach of confidentiality by a Board member is removal from the Board following due consideration by the FRC Nominations Committee. In addition a Board Member may have committed a criminal offence under section 1224B (see above).

Staff and former Staff

2.5. There are similar obligations on staff of the Financial Reporting Council, including AQR staff that they must keep confidential all unpublished information they acquire through their role at the FRC, unless the disclosure of that information has been properly authorised.

2.6. A member of staff in breach of the confidentiality requirements in their employment contract would be subject to the FRC's Disciplinary Procedures. The confidentiality provisions continue to apply following the end of employment and we would consider taking legal action in response to a breach by a former member of staff. In addition, they may have committed a criminal offence under section 1224B (see above).

3. Information Systems and Controls Relating to the Security of Information

3.1. The Conduct Division and the FRC attach great importance to systems and practices designed to protect the confidentiality, integrity and availability of the confidential information that is held. These arrangements cover both the security of physical documents and information held in electronic form and are intended to meet the UK's Seventh Principle of Data Protection; that the measures employed ensure a level of security appropriate to the nature of the data to be protected and the harm that might result from any unauthorised or unlawful processing, as well as accidental loss or destruction or damage to any personal data.

Protecting Physical Documents in the FRC Offices

3.2. The FRC offices are located on a single floor of an office building, which has security guards at the entrance and security patrols that operate throughout the building outside office hours, seven days a week. The FRC offices have restricted access with card access readers on the perimeter doors and a further reader on the door that separates meeting rooms from the offices themselves. The FRC requires that all staff have picture identification badges. Visitors to the FRC must wear temporary identification badges and are escorted at all times within the office area.

The FRC facilities are also protected by fire detection, alarming and suppression systems.

3.3. Any documents provided by CPAB to the FRC in accordance with the Memorandum of Understanding will be kept in a locked cabinet when not in use. Confidential physical documents that are no longer required are disposed of in locked bins for shredding and secure disposal.

Protecting Physical Documents away from the FRC Offices.

3.4. FRC staff may only take confidential documents out of the FRC offices when necessary and are reminded that they need to take great care to protect both the physical document and the content.

3.5. Protecting confidential information away from the FRC offices is of particular importance for staff of the AQR, whose work is largely conducted at the major audit firms, who are responsible for providing secure accommodation and storage facilities for IT equipment and documents.

Protection of Confidential Electronic Information

3.6. All members of staff are bound to follow the FRC IT Security policy, which forms part of their terms and conditions of employment. All Managers monitor their staff and report any IT Security concerns to the Head of IT. The FRC outsources the running of a fully managed IT service on its behalf and any suspicious matters are escalated to the Head of IT. Information held electronically is protected by a system of passwords which governs all network access accounts and enforces password complexity and change frequency requirements. Each individual authorised to access information and documents has a unique user name and password. This username and password combination is required to authenticate the individual requesting information to the computer, application or network environment providing the information. User names are generally not private information whereas the password must be held in strict confidence by each individual. The arrangements dictate the minimum length, complexity and length of validity of a password, enforced through technical controls at the application and operating system levels.

3.7. Passwords do not provide access to all levels of the system. A system of access control grants access to employees through the line management chain of command as is necessary to enable the individual to do his or her job. All access permissions are promptly revoked when an individual ceases to be an employee or contractor. All Passwords are changed every 30 days and complex passwords are in use. If a password is not changed, then network access is withdrawn until the password is changed. All users are locked out of the network after three failed attempts.

3.8. All users have the ability to create 256bit encrypted zip files to protect individual files or folders so that they remain secure when they are emailed or carried on removable media. The AQR uses a separate proprietary electronic audit management system that maintains all the work programmes and documentation relating to audit inspection. The system cannot be accessed by staff from other units within the FRC and is subject to separate password controls.

3.9. Electronic information is further protected by a screen-saver policy, such that all FRC computers activate a screen-saver after 30 minutes of inactivity, which then requires the user's password to be re-entered in order to continue.

3.10. The FRC server room within the office has separate tightly restricted access, which is reviewed regularly. All of the computer systems are protected by UPS and alerting has been setup to inform the Service desk of any power related issues. The Server Room is air-conditioned and has N+1 resilience and would cope with a single AC unit failure. All FRC data is backed up daily and Backup tapes are removed off site twice a week and are password protected. All remaining tapes are stored in a locked cupboard on-site. The FRC is currently reviewing a cloud based solution. The solution is approved to Impact Level (IL2). The Impact

Levels are defined by the Cabinet Office and the National Technical Authority for Information Assurance for UK Government. The solution has an up time of 99% and is approved for use by Governmental departments.

3.11. The system also provides for the generation of a security audit trail that contains information to enable the investigation of a loss of data or improper access to data. In particular, the system associates user identification information with any system request or activity, so that the initiating user can be held accountable for that request or activity. Audit logs are enabled at the operating system. Individual account identifications are tied to the operating system to ensure proper accountability. Network access activity logs are maintained and reviewed regularly for inappropriate access.

3.12. In addition, all IT assets (for example desktop and laptop computers, computer files, electronic mail) are the property of the FRC and subject therefore to specific controls. For example, these prevent the installation of unauthorised software on any FRC computer and ensure that all data held on laptops that are used outside the FRC offices include a high level of encryption for all data. All handheld devices and laptops are encrypted and all users are forced to change the encryption passwords every 30 days.

3.13. All applications and operating systems have security flaws and the FRC has a policy of applying security patches in a timely manner to applications and operating systems, as these flaws are identified. This helps to ensure that applications and operating systems are protected from the threat of hacking, cracking and malware attacks by repairing any known security flaws. Regular monthly patching of the Server and Desktop/Laptop estate takes place as part of the managed service by the service provider. In terms of email exchange this is captured by the Websense service. All IT Security breaches are reported to the Head of IT who will then take any necessary action. The patch management process is initiated on a monthly basis and incorporates the following steps:

- Identification of patches to be applied
- Evaluation of risk and establishment of patch priority
- Patch testing
- Patch deployment

3.14. The FRC also uses software tools such as Intrusion Prevention systems/ Improvement Detection Systems (IPS/ IDS), firewalls, anti-malware and anti-virus system software to protect its IT resources from malicious access. All emails are scanned and cleaned externally before they are delivered to the FRC infrastructure.

3.15. FRC staff must take appropriate steps to limit the risk of the introduction of malicious code. In particular, they are prohibited from disabling any anti-virus software and must always follow proper policy and procedures when downloading and installing files or software on any IT assets in their custody. A staff member who fails to follow these requirements and whose conduct disrupts the normal operation of the FRC's IT systems is liable to disciplinary action, which includes the possible termination of employment.

3.16. To access the FRC Network remotely, all users require a User name, their network password, Pin details and a number generating security token. If any one of these factors is incorrect, then the user will not gain access to the Network.

3.17. SSL technology is used by the FRC to safeguard the data that is held on its website. We do not store any confidential data on the website and our internal systems are protected by multiple layers of authentication when they are accessed remotely. We do not currently

have a regular programme of risk/vulnerability assessments, as there is very little change to our infrastructure and we believe the regular patching deals with all threats. We have recently carried out a Security test of our Infrastructure and there were no major issues.

March 2015